基于 IFCM 加权的 SVDD 硬件木马检测方法 *

魏延海 [1]，李雄伟 [1]，张　阳 [1]，胡晓阳 [1]，张坤鹏 [2]

(1. 陆军工程大学石家庄校区 装备模拟训练中心，石家庄 050003; 2. 中国人民解放军 66407 部队，北京 100093)

摘　要：针对硬件木马（hardware Trojan，HT）种类繁多难以获取未知木马特征及采集的旁路信号含噪声问题，提出了一种基于 IFCM 加权的 SVDD（IFCMW_SVDD）硬件木马检测方法。传统支持向量数据描述（SVDD）在解决单分类问题时存在相同条件下训练全部样本的不足，需要根据相应问题对样本有主次之分进行训练。通过一种改进的模糊 C 均值方法（IFCM）计算"金片"旁路信号的隶属度，将其作为样本特征的权重（W）系数，使得针对硬件木马检测问题构建 SVDD 模型的支持向量能够描述"金片"信号的同时尽可能减小描述范围。实验表明，所提方法实现单分类硬件木马检测的同时较传统 SVDD 算法在检测精度和稳定性上都有所提高。

关键词：硬件木马；旁路信号；改进模糊 C 均值算法；支持向量数据描述；隶属度

中图分类号：TN918　　doi: 10.3969/j.issn.1001-3695.2018.05.0315

Hardware Trojan detection method based on IFCM weighted SVDD

Wei Yanhai[1], Li Xiongwei[1], Zhang Yang[1], Hu Xiaoyang[1], Zhang Kunpeng[2]

(1. *Equipment Simulation Training Center, The Army Engineering University of PLA, Shijiazhuang Campus, Shijiazhuang* 050003, *China*; 2. *Unit* 66407 *of PLA*, *Beijing* 100093, *China*)

Abstract: This paper proposed a hardware Trojan (HT) detection method based on IFCM Weighted SVDD (IFCMW_SVDD) aimed at solving the problem that a great variety of Hardware Trojans that is difficult to obtain unknown Trojan Features characteristics, and the collected Side-channel signal contains noise problems. The traditional Support Vector Data Description (SVDD) has the defective of training all the samples of the same conditions when solving the single classification problem, samples need to be divided into primary and secondary parts according to their problems and trained. But this algorithm calculates the membership degree of the "gold chip " bypass signal by Improved Fuzzy C-means Method (IFCM) , and uses it as the Weight (W) coefficient of the sample feature , the support vectors of constructed SVDD model for the Hardware Trojan detection problem can describe the "golden chip" signals while minimizing the description range. Experiments show that the method proposed to this paper achieves the detection of single-class Hardware Trojans and has higher detection accuracy and stability than the traditional SVDD algorithm.

Key words: hardware Trojan; side-channel signals; improved fuzzy C-means method (IFCM); support vector data description (SVDD); membership degree

0　引言

随着集成电路（IC）市场需求量的不断加大，芯片厂家为降低其生产成本大都将电路设计、芯片制造和封装等过程分离并进行外包生产制造，IC 越来越容易被植入硬件木马而受到恶意攻击。硬件木马是通过篡改 IC 原有设计达到某种恶意功能的微小电路模块，具有很强的隐蔽性。为保证 IC 应用的安全性，针对 IC 的硬件木马检测问题已成为当前的研究热点。

目前，面向硬件木马检测的方法有基于逆向工程芯片解剖、逻辑功能测试技术和旁路分析技术等。利用逆向解剖技术对硬件木马的检测率可以达到 100%[1]，但是整个过程耗时费力；而基于芯片旁路信号的检测技术不需要对芯片做开片处理[2]，通过获取其旁路信号并进行特征变换作差异对比即可判别待测 IC 是否被植入硬件木马。然而，当前基于旁路信号检测技术大多是针对实验需求设计的木马提出的，一种检测方法只对应某类木马进行检测[3]，而对于未知木马和一对多的问题检测效果并不理想。Bao 等人[4]提出了一种反向工程方法来识别不含硬件木马的芯片，并采用一类支持向量机（one-class SVM，

收稿日期：2018-05-03；**修回日期：**2018-06-21　**基金项目：**国家自然科学基金资助项目（61271152, 51377170）；国家青年科学基金资助项目（61602505）；河北省自然科学基金资助项目（F2012506008）

作者简介：魏延海（1993-），男，山东五莲人，硕士，主要研究方向为信息安全研究；李雄伟（1975-），男，河北定州人，教授，硕导，博士，主要研究方向为信息安全（lxw-wys@163.com）；张阳（1984-），男，讲师，博士研究生，主要研究方向为密码学；胡晓阳（1994-），男，吉林九台人，硕士，主要研究方向为旁路攻击；张坤鹏（1988-），男，河南商丘人，助理工程师，主要研究方向为信息安全保密．

OCSVM）来构建硬件木马检测模型。但由于构建模型所用样本受环境影响，从而扩大所构建模型的范围而造成过拟合问题。徐晶等人[5]建立一种基于 SVDD 算法与聚类算法相结合的入侵检测模型，首先将正常样本通过 *k* 均值（又名 *C* 均值）算法进行聚类处理，再进行数据描述达到检测异常数据的目的。虽然该方法采用 DAPRA.99(美国国防部高级计划研究局)样本进行实验取得了较好检测效果，但针对木马信号等易受噪声影响并相对复杂的样本很难得到较高的检测率。Niazmardi 等人[6]设计了一种基于 SVDD 与 FCM 算法解决遥感图像缺乏足够高质量训练数据和高维高光谱数据的问题，但 FCM 容易将一类相对离散的样本判别为多个类别。基于上述问题，通过分析实验所采集的高维空间中服从正态分布旁路信号样本，考虑到 SVDD 可处理异常数据的特点，为弥补 FCM 针对单聚类中心离散和传统 SVDD 训练复杂度高的不足，本文采用 IFCM 对 SVDD 建模进行加权处理，在传统 SVDD 实现单分类硬件木马检测的基础上进行改进。实验表明，改进的 SVDD 模型针对多种未知木马仍具有良好的检测效果，能够在无须获取木马相关特性的前提下实现多种木马的检测。

1　功耗检测模型及相关问题分析

旁路信号大多为电路的电磁、功耗信号，其中功耗信号相比前者有更高的准确性而成为硬件木马检测的主流研究对象。实际操作中采集的每条功耗信号是根据设置的采样点数量 *n* 测得芯片在不同时刻的功耗大小数据集,设采样次数为 *m*，则可得到功耗矩阵 $X_{m\times n}$，每条信号 *n* 维的向量，则可以视为在空间中由协方差矩阵和均值所决定的相关样本点，形似为超椭球。

经过大量实验验证分析得知，所测“金片”功耗电流信号（I_g）由干路电流（I_e）和噪声（I_n：电子噪声 I_{el}、转换噪声 I_{sw}）电流组成：$I_g=I_e+I_n$、$I_n=I_{el}+I_{sw}$，则待测芯片（含硬件木马信号 I_{tr}）信号 I_g 可表示为： $I_g=I_e+I_n+I_{tr}$。基于旁路信号检测的思路是分别检测“金片”和待测芯片（含木马）的旁路信号，当硬件木马占芯片电路开销较高的时，相对应的 I_{tr} 值较大，通过观测波形进行判别“金片”信号与木马信号；当开销较低时，虽然可以忽略 I_n 的影响，但是传统方法不能将两者进行有效区分，则需要借助 K_L 投影[7]、 K-means 聚类分析[8,9]等相关方法进行信号特征分析查找两者之间的特征差异，从而达到检测芯片的目的。但当木马规模更小时，K_L 方法无法找到一组有效的正交投影方向进行区分。另外 K-means 聚类面对类间距较小、两类样本重叠等问题依然难以进行有效判别，这时 SVDD 算法就体现出将样本向更高维空间映射进行分类的优越性，最重要的是只需使用“金片”信号即可进行相关检测工作。

2　一种基于 IFCM 加权的 SVDD 算法

2.1　IFCM 算法

在硬件木马检测中，传统 *C* 均值算法（*C-means*）将 *n* 条信号样本划分到最初设定的 *c* 个类别中，使每个样本与其所在样本类均值的误差平方和最小，从而使式（1）准则函数最小。

$$J_e=\sum_{i=1}^{c}\sum_{y\in\Gamma_i}\|y-m_i\|^2 \tag{1}$$

其中：m_i 为第 *i* 类的均值；$y\in\Gamma_i$ 是分到 *i* 类的所有样本。*C-means* 算法属于硬分类方法，强行分类致使分类效果不理想[10]。而模糊 *C* 均值（FCM）试图将分类进行模糊化，缓解硬分类问题，则可以将相关问题进行重新描述：假设$\{x_i，i=1,2,\ldots n\}$是 *n* 条信号组成的样本集合，*C*（本文只针对“金片”样本则取值为 1）为预定的类别数目，$\{m_i，i=1,2,\ldots c\}$是每簇训练样本的中心位置，$\mu_j(x_i)$作为第 *i* 个训练样本点作用 *j* 类的隶属度函数，聚类损失函数可重新改写为

$$\min J_f=\sum_{i=1}^{c}\sum_{y\in\Gamma_i}\left[\mu_j(x_i)\right]^b\|x_i-m_j\|^2 \tag{2}$$

其中：指数 *b* 是大于 1 的聚类结果模糊程度的控制常数。依据式（2）可知，随着 *b* 取值逐渐增大，其模糊程度越大；当 $b\rightarrow\infty$，则该算法得到的是完全模糊的解，说明各类别的中心点都收敛到了全部训练样本的中心，全部参与训练的样本属于各类的概率相等，因此，根据经验将 *b* 的值取 2 左右。不同模糊聚类算法是由式（1）决定。FCM 算法，对于隶属度的约束为

$$\sum_{j=1}^{c}\mu_j(x_i)=1, i=1,2,\cdots,n \tag{3}$$

而 IFCM 为克服 FCM 使离散点根据式（3）的规定对各类的隶属度值较大而影响迭代效果的不足，规定所有的训练样本对每类的隶属度总和为 *n*。

$$\sum_{j=1}^{c}\sum_{i=1}^{n}\mu_j(x_i)=n \tag{4}$$

在式（4）条件制约下使得式（2）极小，则令其对隶属度$\mu_j(x_i)$和中心 m_i 求偏导为 0，可得

$$\frac{\partial J_f}{\partial m_i}=0;\frac{\partial J_f}{\partial\mu_j(x_i)}=0\Rightarrow\begin{cases}m_j=\dfrac{\sum_{i=1}^{n}\left[\mu_j(x_i)\right]^b x_i}{\sum_{i=1}^{n}\left[\mu_j(x_i)\right]^b}, j=1,2,\cdots,n\\ \mu_j(x_i)=\dfrac{\left(1/\|x_i-m_j\|^2\right)^{1/(b-1)}}{\sum_{k=1}^{c}\sum_{l=1}^{n}\left(1/\|x_l-m_k\|^2\right)^{1/(b-1)}}\end{cases} \tag{5}$$

$$s.t. i=1,2,\cdots,n,\ \ j=1,2,\cdots,c$$

综上所述，IFCM 算法步骤描述如下：

算法I
a)设定信号聚类数目 *c* 和参数 *b*；
b)利用 C 均值算法求得的 m_i，初始化 m_i；
c)循环操作以下运算，当各个样本的隶属度值稳定结束操作；
(a)利用 m_i 依据式（5）计算隶属度函数；
(b)利用(a)所求按照式（5）$\mu_j(x_i)$计算并更新各类聚类中心。

2.2　SVDD 算法分析

SVDD 算法是在支持向量机（SVM）的基础上针对单分类问题提出的算法，特点是只需要目标样本训练而不考虑非目标样本（木马信号）。目前已经在图像模式识别[6]、设备故障分析[11,12]等研究领域取得了理想应用。根据分析“金片”旁路功耗

信号（目标样本）的空间分布特点，符合 SVDD 算法训练样本构建模型标准。SVDD 基本原理是将有限的训练样本通过映射函数 Φ 映射到更高维空间，根据实际问题需求建立能够尽可能包含训练样本与将异常样本排除在外的最小超球体，达到检测的目的。SVDD 的目标函数描述如下：

$$\begin{aligned}&minR^2+\lambda\sum_{i=1}^{n}\xi_i\\&s.t.\|\phi(x_i)-c\|^2\le R^2+\xi_i,\xi_i\ge 0\end{aligned} \quad (6)$$

其中：R 表示超球体的半径；λ 为大于零的惩罚系数，随着 λ 值不断减小，训练模型包含的“金片”信号样本越少，需要对模型大小与检测正确率进行折衷处理；ξ_i 是松弛因子，其作用是衡量非目标点或者噪声样本重要程度；c 作为球心。

式（6）作为凸二次规划问题，对该约束条件添加拉格朗日乘子 $\alpha_i,\beta_i\ge 0$ 可得

$$\begin{aligned}&L(R,a,\alpha_i,\xi_i)=R^2+\lambda\sum_{i=1}^{n}\mu_i\xi_i-\\&\sum_{i=1}^{n}\alpha_i(R^2+\xi_i-\|\phi(x_i)-c\|^2)-\sum_{i=1}^{n}\beta_i\xi_i\end{aligned} \quad (7)$$

令 $L(R,a,\alpha_i,\xi_i)$ 对 R 与 ξ_i 分别求偏导为 0 以求得最小值，可得

$$\frac{\partial L}{\partial R}=0,\frac{\partial L}{\partial \xi_i}=0\Rightarrow\begin{cases}\sum_{i=1}^{n}\alpha_i=1\\ \alpha_i+\beta_i-\lambda=0\end{cases} \quad (8)$$

因此将（8）代入式（7）可得其“对偶问题”：

$$\begin{aligned}&max\sum_{i=1}^{n}\alpha_iK(x_i,x_i)-\sum_{i=1}^{n}\sum_{j=1}^{n}\alpha_i\alpha_jK(x_i,x_j)\\&s.t.\lambda\ge\alpha_i\ge 0,i=1,2,\cdots,n,j=1,2,\cdots,n\end{aligned} \quad (9)$$

其中：$K(x_i,x_j)=\phi(x_i)^{\mathrm{T}}\phi(x_i)$，超球体的支持向量为样本点 $\lambda>\alpha_i>0$ 的点，α_i 说明该样本点被包含在球体内；根据分析可知球心和支持向量点（x_f）到球心的距离分别为

$$\begin{cases}c=\sum_{i=1}^{n}\alpha_i\phi(x_i)\\ R=\sqrt{K(x_i,x_i)-2\sum_{i=1}^{n}\alpha_iK(x_i,x_f)+\sum_{i,j=1}^{n}\alpha_i\alpha_jK(x_i,x_j)}\end{cases} \quad (10)$$

任意样本点可利用式（10）进行计算与样本中心 c 的距离 R_i；若 $R_i\le R$ 该样本点为“金片”信号，否则为含木马信号。

2.3　基于 IFCM 加权的 SVDD 检测模型

采用传统 SVDD 训练功耗信号样本选择支持向量时，面对样本点无层次之分，而采集的“金片”旁路信号含噪声等离散样本使得训练样本中心偏离，故引入隶属度 $\mu_j(x_i)$作为 SVDD 训练样本的加权参数 W_i（样本点越接近聚类中心，其隶属度越大），以提高 SVDD 训练模型硬件木马检测率。则（6）式可改写为

$$\begin{aligned}&\min R^2+\lambda\sum_{i=1}^{n}W_i\xi_i\\&s.t.\|\phi(x_i)-c\|^2\le R^2+\xi_i,\xi_i\ge 0\end{aligned} \quad (11)$$

加权后的式（7）变为

$$\begin{aligned}&L(R,a,\alpha_i,\xi_i)=R^2+\lambda\sum_{i=1}^{n}W_i\xi_i-\\&\sum_{i=1}^{n}\alpha_i(R^2+\xi_i-\|\phi(x_i)-c\|^2)-\sum_{i=1}^{n}\beta_i\xi_i\end{aligned} \quad (12)$$

对式（12）求(R,c,ξ_i)偏导数并令其为零，把所求代入式（12）可得对偶式：

$$\begin{aligned}&max\sum_{i=1}^{n}\alpha_iK(x_i,x_i)-\sum_{i=1}^{n}\sum_{j=1}^{n}\alpha_i\alpha_jK(x_i,x_j)\\&s.t.\lambda W_i\ge\alpha_i\ge 0,i=1,2,\cdots,n,j=1,2,\cdots,n\end{aligned} \quad (13)$$

经计算求得的式（10）结果不变。通过对比分析式（6）～（13）可知，加入加权参数后改变的只是参数 α_i，进而说明隶属度值大的信号样本与之对应的拉格朗日系数较大，从而在构建 SVDD 木马检测模型中成为支持向量的可能性相对较大，构建的模型更具合理性。

综上所述，基于 IFCM 的 SVDD 算法步骤描述如下：

算法II

a)输入功耗信号样本 $X=\{x_i，i=1,2，…n\}$；设定聚类数目 $c=1$ 和参数 $b=2$。

b)对集合 X 做十条一平均，求得处理后的数据矩阵。

c)利用 C 均值算法求得的 m_i，初始化 m_i。

d)循环操作以下运算，当各个样本的隶属度值稳定结束操作：

　(a)利用 m_i 依据式（5）计算隶属度函数；

　(b)利用①所求按照式（5）计算 $\mu_j(x_i)$并更新“金片”信号聚类中心。

e)利用样本隶属度对式（7）加权处理。

f)样本标准化处理，构建 SVDD 模型。

g)输入未知信号样本，根据式（10）计算距聚类中心距离进行对比。

h)符合判别式 $R-R_i<0$，则判定该样本含有硬件木木马；反之，不含有硬件木马。

2.4　算法有效性分析

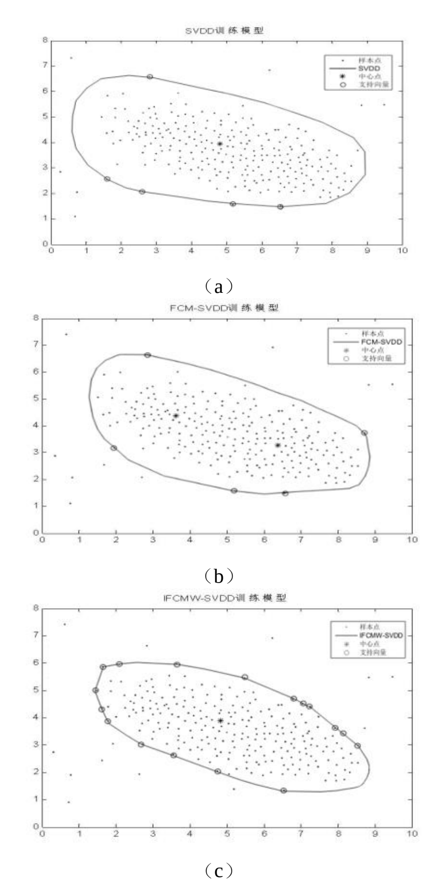
为验证算法有效性，本文通过对二维数据样本进行训练建立模型。对于相同的训练样本模拟实验结果如图 1 所示。

在训练过程中选择应用最广泛的高斯核函数：$Kernel(x_i,x_j)=e^{(-\|X-X'\|/2\sigma^2)}$，采用经典网格寻优算法对参数组合$(\lambda,\sigma^2)$进行寻优，设置寻优范围：$\lambda=[10^{-8},2^7]$、$\sigma^2=[10^{-5},2^{-4}]$和参数初始值：$\lambda=2$、$\sigma^2=10^{-5}$。其中图 1（a）（b）和（c）分别为 SVDD、FCM_SVDD 和 IFCMW_SVDD 模型。由图 1 可知，与 SVDD 和 FCM_SVDD 模型相比，IFCMW_SVDD 范围小、支持向量点多于前两者并且选择更加合理；同时 FCM_SVDD 有两个中心点，表示将该类样本视为两类，而 IFCMW_SVDD 实验显示只有一个中心点，弥补了前者的不足之处。

3　物理实验验证

3.1　实验配置

为验证本文提出的检测方法能够检测多种木马，实验 1 采用 ISCAS85 电路进行仿真，根据其所含电路大小各式各样的特点，可以设置不同规模的硬件木马满足实验需求。本文分别在其 c1908、c2670、c3540、c5315、c6288 和 c7552 电路设计了不同门数大小的组合型硬件木马，其结构原理如图 2 所示。



（a）

（b）

（c）

图 1　不同算法在相同条件下的训练模型

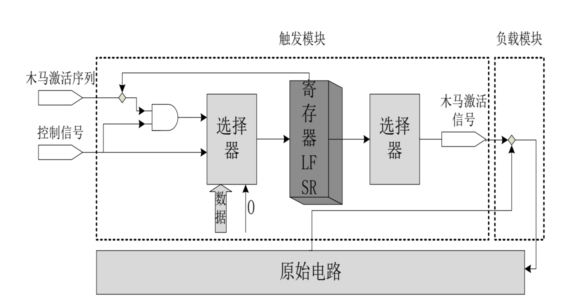


图 2　硬件木马结构原理

该木马包括触发模块和负载模块两部分。当控制信号为低电平时，寄存器被数据重置初始状态；为高电平时，寄存器处于工作状态向选择器输出数据。当寄存器为处于某一终态时，木马激活信号被置为高电平，此时负载模块被触发。分别进行“金片”信号和“木马”信号采集（时间分辨率为 2PS；仿真时间为 1.4 ms）。为尽量减少噪声对所采集的信号质量影响，提高采样次数 m 并进行平均 10 次处理。

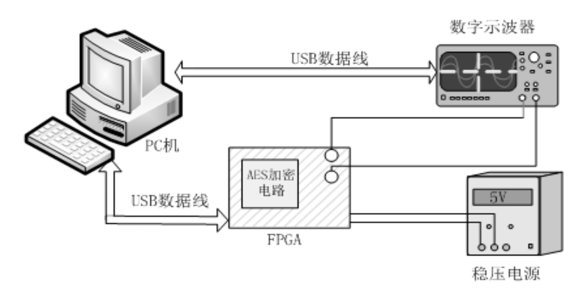


图 3　采集旁路信号物理实验原理

为进一步验证方法的有效性，实验 2 采用 SASEBO 开发板采集所需的旁路信号。物理实验平台原理如图 3 所示。其中通过开发板的 FPGA 进行运行加密算法（植入硬件木马采集“木马”信号），利用示波器（型号为 Tektronix DPO4032；带宽为 350 MHz）进行“金片”信号采集，传至采集 PC 机（CPU i5-6400 2.70 Hz 8 GB 内存）测试向量，稳压电源设置为 5V；Eclipse+Pydev+Anaconda3 作为 SVDD、IFCM 样本训练编程环境；同时利用 MATLAB 进行模型评估。

3.2　实验结果分析

通过实验 1 对“金片”信号与“木马”信号采集，分别采集 1 000 条采样点为 600 点的功耗信号；为充分验证本文方法有效性，实验 2 设置采集 5 000 条采样点为 10 000 点的功耗信号，并分别随机选择两类信号其中各 10 条进行对比（实验 1：600 采样点；实验 2：1 400 采样点），如图 4、5 所示。

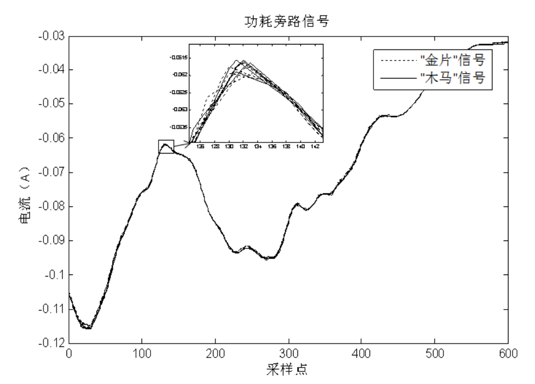


图 4　ISCAS85 电路功耗信号

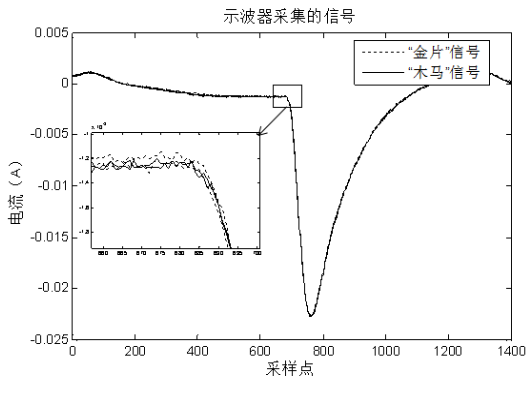


图 5　FPGA 旁路信号

对两次实验采集的两种信号进行对比分析得知，两种信号虽然在某些采样点存在一定差异，但总体波动微小，直接观察不能明显区分两种信号，无法实现硬件木马检测。

表 1　不同规模下各算法检测率

电路	门数	硬件木马门数 15：面积开销（%）	15：检测率/% SVDD	15：检测率/% IFCMW_SVDD	硬件木马门数 6：面积开销（%）	6：检测率/% SVDD	6：检测率/% IFCMW_SVDD
c1908	1042	1.44	65.12	99.54	0.57	61.03	96.48
c2670	1389	1.08	63.86	97.21	0.43	58.36	96.12
c3540	1892	0.79	61.25	95.56	0.32	39.47	95.74
c5315	2620	0.57	59.65	95.32	0.23	34.14	89.25

c6288	2416	0.62	62.45	96.64	0.25	36.31	90.36
c7552	4046	0.37	41.88	92.34	0.15	31.25	88.15

通过对实验 1 采集的“金片”信号进行训练，采集 ISCAS85 电路 7 种不同规模的硬件木木马信号进行测试，同时利用传统 SVDD 在同一条件下进行对比实验，测试结果如表 1 所示。分析得知，本文算法检测效果远远好于 SVDD 算法，并且当开销面积为 1.44%时，本文算法检测率高达 99.54%，而后者仅为 65.12%；同时，当随着面积开销不断减小，两者的检测率都有所下降，但与 SVDD 相比有较好的稳定性。

实验 2 在 FPGA 中植入占 AES 加密电路开销 2.5%的硬件木木马，采用 SVDD、FCM_SVDD 和 IFCMW_SVDD 对采集的“金片”信号以 1 000 条为窗长进行分组训练，并采用网格寻优算法进行参数寻优后进行测试。各随着训练样本数变化检测率变化曲线如图 6 所示。由图可知，SVDD 和 FCM_SVDD 检测率总体相近，但远远低于本文算法。

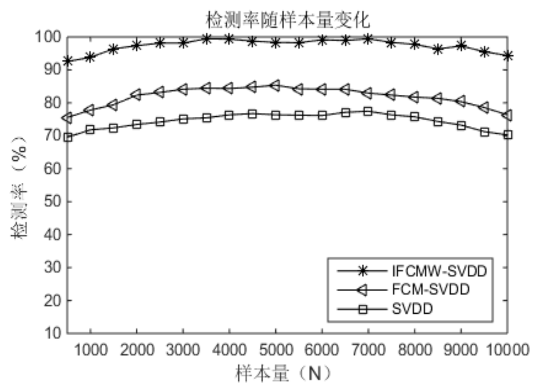


图 6　不同算法检测率随样本量变化

为进一步验证经本文方法所改进模型的有效性，本文采用查准率（*P*）、查全率（*R*）和 “*P-R*” 图方法对模型进行评估。其定义式为

$$P = TP / (TP + FP)$$
$$R = TP / (TP + FN)$$

其中：*TP* 为模型正确判断含木马信号条数（真正例）；*FP* 为模型将不含木马信号误判为含木马的信号条数（假正例）；*FN* 为将含木马信号误判不含木马的信号条数（假反例）；*TN* 为正确判断不含木马信号条数（真反例）。

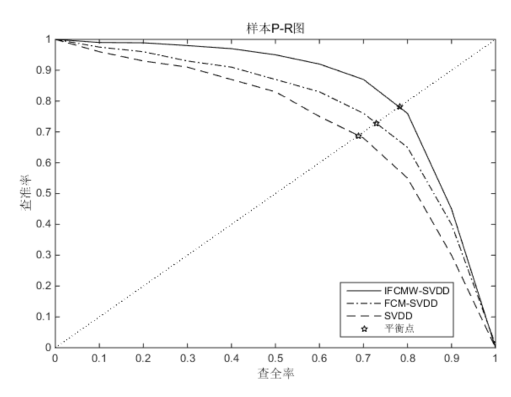


图 7　P_R 曲线

通过对样本查准率和查全率计算，得到两个指标的“*P-R*”图，如图 7 所示。评判标准：若一个模型的 *P-R* 曲线被另一个模型的曲线完全“包住”，则可判定后者性能优于前者性能。经观察 SVDD 算法的 *P_R* 曲线最低，表示三者中性能最差，FCM_SVDD 次之，IFCMW_SVDD 性能最优，同时可以通过度量参数“平衡点”（查准率=查全率）越高性能越好进行评判。传统 SVDD、FCM_SVDD、IFCMW_SVDD 各自“平衡点”依次升高，亦可说明 IFCMW_SVDD 在木马检测实验中优于未加权的 SVDD 和 FCM_SVDD 算法。

4　结束语

本文提出了一种基于 IFCMW_SVDD 硬件木马检测方法，首先基于旁路信号特性分析了 SVDD 算法实现对单分类硬件木马检测的可行性；然后针对 SVDD 训练旁路信号模型检测木马信号存在的过拟合问题，利用改进的 FCM 算法进行加权处理构建适合于硬件木马检测的单分类模型。一般的检测方法不仅要获取相关木马特征，而且需要更多的存储空间。本文方法将样本信号映射到高维空间中，利用支持向量构建超椭球，把含未知木马的旁路信号分离在超椭球外部，从而检测到多种未知木马；同时该方法只需要获取相应的“金片”信号，不对木马信号进行分析；利用加权处理缓解了因训练模型规模偏小（大）造成的过拟合（欠拟合）问题，经训练的模型只保留相关的支持向量点即可，节省了大量存储空间。最后，通过对仿真数据和旁路信号实验验证表明，本文方法对设计的多种硬件木马有较好的检测效果，为下一步的硬件木马检测研究提供了新思路。

参考文献：

[1] Bao Chongxi, Yang Xie, Liu Yuntao, *et al.* Reverse engineering-based hardware trojan detection [M]// The Hardware Trojan War. Berlin: Springer, 2018: 269-288.

[2] 张阳，李雄伟，陈开颜，等. 基于故障注入的硬件木马设计与差分分析 [J]. 华中科技大学学报：自然科学版, 2014, 42 (4): 68-71. (Zhang Yang, Li Xiongwei Chen Kaiyan, *et al.* Research of hardware trojan designand differential analysis based on fault injection [J]. Journal of Huazhong University of Science and Technology: Natural Science Edition, 2014, 42 (4): 68-71.)

[3] Dupuis S, Flottes M L, Di Natale G, *et al.* Protection against hardware trojans with logic testing: proposed solutions and challenges ahead [J]. IEEE Design & Test, 2018, 35 (2): 73-90.

[4] Bao Chongxi, Forte D, Srivastava A. On application of one-class SVM to reverse engineering-based hardware trojan detection [C]// Proc of the 15th International Symposium on Quality Electronic Design. Piscataway, NJ: IEEE Press, 2014: 47-54.

[5] 徐晶，石端银，张亚江，等. 基于聚类和 SVDD 的一类入侵检测模型 [J]. 控制与决策, 2010, 25 (3): 441-444. (Xu Jing, Shi Duanyin, Zhang Yajiang, *et al.* Model of IDS based on SVDD and cluster algorithm [J]. Control and Decision, 2010, 25 (3): 441-444.)

[6] Niazmardi S, Homayouni S, Safari A. An improved FCM algorithm based

on the SVDD for unsupervised hyperspectral data classification [J]. IEEE Journal of Selected Topics in Applied Earth Observ ations & Remote Sensing, 2013, 6 (2): 831-839.

[7] Agrawal D, Baktir S, Karakoyunlu D, *et al*. Trojan detection using IC fingerprinting [C]// Proc of Symposium on Security and Privacy. Washington DC: IEEE Computer Society , 2007: 296-310.

[8] 王柏人，曲鸣. 基于 K-means 聚类分析的硬件木马检测方法 [J]. 北京电子科技学院学报，2016, 24 (2): 84-87. (Wang Bairen, Qu Ming. Hardware trojan detection method based on K-means clustering analysis [J]. Journal of Beijing Electronic Science and Technology Institute. 2016, 24 (2): 84-87.)

[9] Bao Chongxi, Forte D, Srivastava A. On reverse engineering-based hardware trojan detection [J]. IEEE Trans on Computer-Aided Design of Integrated Circuits and Systems, 2018, 35 (1): 49-57.

[10] 边肇祺，张学工. 模式识别 [M]. 2 版. 北京：清华大学出版社，2000. (Bian Zhaoqi, Zhang Xuegong. Pattern recognition [M]. 2nd Edition. Beijng: Tsinghua University Press, 2000.)

[11] Gryllias K, Qi Junyu, Mauricio A R, *et al*. A semi-supervised SVDD-based fault detection method for rolling element bearings [C]// Proc of the 1st World Congress on Condition Monitoring. 2017.

[12] Chen Muchen, Hsu Chunchin, Malhotra B, *et al*. An efficient ICA-DW-SVDD fault detection and diagnosis method for non-Gaussian processes [J]. International Journal of Production Research, 2016, 54 (17): 1-11.